

## REMARKS

This is a full and timely response to the outstanding non-final Office Action mailed November 5, 2007. Upon entry of the amendments in this response, claims 1 – 14 remain pending. In particular, Applicants amend claims 1, 3 – 6, 10, and 13 and add claims 15 – 20. Reconsideration and allowance of the application and presently pending claims are respectfully requested.

### **I. Rejections Under 35 U.S.C. §103 – *Feldman* in view of *Anderson***

#### **A. Claim 1 is Allowable Over *Feldman* in view of *Anderson***

The Office Action indicates that claim 1 stands rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent Number 6,069,889 ("*Feldman*") in view of U.S. Publication Number 2003/0014665 ("*Anderson*"). Applicants respectfully traverse this rejection for at least the reason that *Feldman* in view of *Anderson* fails to disclose, teach, or suggest all of the elements of claim 1. More specifically, claim 1 recites:

A secure data switching node comprising:  
a. a plurality of communications ports;  
b. a switching database having a plurality of switching entries, each one of the plurality of switching entries specifying an association between a data network node identifier and a communications port;  
c. a plurality of switching entry protection flags, corresponding to the plurality of switching entries, ***each of the plurality of switching entry protection flags configured with a predetermined value that determines whether each of the switching entries is protected from update***; and  
d. a controller executing a secure switching database update process, for at least one of the switching entries, ***wherein executing a secure switching database update process includes determining, from at least one of the switching entry protection flags, whether the at least one of the switching entries is protected from update***, whereby an attempt by a hostile data network node to effect a modification of a protected switching entry is prevented when the protection flag is set, enabling the data switching node to operate securely concurrently in friendly and hostile data networking environments.

***(emphasis added)***

Applicants respectfully submit that claim 1, as amended, is allowable over the cited art for at least the reason that neither *Feldman* nor *Anderson*, alone or in combination, discloses, teaches, or suggests a “secure data switching node comprising... a plurality of switching entry protection flags, corresponding to the plurality of switching entries, ***each of the plurality of switching entry protection flags configured with a predetermined value that determines whether each of the switching entries is protected from update...wherein executing a secure switching database update process includes determining, from at least one of the switching entry protection flags, whether the at least one of the switching entries is protected from update***” as recited in claim 1, as amended. More specifically, the Office Action admits that *Feldman* “fails to teach a plurality of switching entry protection flags...” (OA page 3, element 6). For at least this reason, claim 1, as amended, is allowable.

Additionally, *Anderson* fails to overcome the deficiencies of *Feldman*. More specifically, *Anderson* discloses “[o]nce notification is received, an Internet host establishes a security authentication with an upstream router from which attack traffic is received. Once security authentication is established, the Internet host transmits one or more squelch filters to the upstream router” (page 2, paragraph [0025]). Applicants respectfully submit that this is different than claim 1, as amended, for at least the reason that the squelch filters are not transmitted to a location for implementation until after authentication is established. Consequently, *Anderson* cannot disclose switching entry protection flags that have a predetermined value that determine whether each of the switching entries is protected from update. For at least this additional reason, claim 1, as amended, is allowable.

**B. Claim 3 is Allowable Over *Feldman* in view of *Anderson***

The Office Action indicates that claim 3 stands rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent Number 6,069,889 (“*Feldman*”) in view of U.S. Publication Number 2003/0014665 (“*Anderson*”). Applicants respectfully traverse this rejection for at least

the reason that *Feldman* in view of *Anderson* fails to disclose, teach, or suggest all of the elements of claim 3. More specifically, claim 3 recites:

A secure data switching node comprising:  
a. a plurality of physical communications ports;  
b. a switching database having a plurality of switching entries, each one of the plurality of switching entries specifying an association between a data network node identifier and a communications port;  
c. a plurality of topology discovery disable flags, corresponding to the plurality of switching entries, ***each of the plurality of topology discovery disable flags configured with a predetermined value that determines whether additional switching entries are prevented from being added to the switching database***; and  
d. a controller executing a secure data transport network topology update process for at least one of the switching entries, ***wherein executing a secure data transport network topology update includes determining, from at least one of the topology discovery disable flags, whether switching entries are prevented from being added to the switching database***, whereby attempts by a hostile data network node to effect at least one addition of a switching entry specifying a communications port associated with a topology discovery disabled physical communications port are prevented, enabling the data switching node to operate securely concurrently in friendly and hostile data networking environments.

***(emphasis added)***

Applicants respectfully submit that claim 3, as amended, is allowable over the cited art for at least the reason that neither *Feldman* nor *Anderson*, alone or in combination, discloses, teaches, or suggests a “secure data switching node comprising... a plurality of switching entry protection flags, corresponding to the plurality of switching entries, ***each of the plurality of topology discovery disable flags configured with a predetermined value that determines whether additional switching entries are prevented from being added to the switching database... wherein executing a secure data transport network topology update includes determining, from at least one of the topology discovery disable flags, whether switching entries are prevented from being added to the switching database***” as recited in claim 3, as amended. More specifically, the Office Action admits that *Feldman* “fails to teach a plurality of switching entry protection flags...” (OA page 3, element 6). For at least this reason, claim 3, as amended, is allowable.

Additionally, *Anderson* fails to overcome the deficiencies of *Feldman*. More specifically, *Anderson* discloses “[o]nce notification is received, an Internet host establishes a security authentication with an upstream router from which attack traffic is received. Once security authentication is established, the Internet host transmits one or more squelch filters to the upstream router” (page 2, paragraph [0025]). Applicants respectfully submit that this is different than claim 3, as amended, for at least the reason that the squelch filters are not transmitted to a location for implementation until after authentication is established. Consequently, *Anderson* cannot disclose determining whether additional switching entries are prevented from being added to the switching database. For at least this additional reason, claim 3, as amended, is allowable.

**C. Claim 4 is Allowable Over *Feldman* in view of *Anderson***

The Office Action indicates that claim 4 stands rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent Number 6,069,889 (“*Feldman*”) in view of U.S. Publication Number 2003/0014665 (“*Anderson*”). Applicants respectfully traverse this rejection for at least the reason that *Feldman* in view of *Anderson* fails to disclose, teach, or suggest all of the elements of claim 4. More specifically, claim 4 recites:

A secure data switching node comprising:  
a. a plurality of physical communications ports;  
b. a switching database having a plurality of switching entries, each one of the plurality of switching entries specifying an association between a data network node identifier and a communications port;  
c. a plurality of topology discovery disable flags, corresponding to the plurality of switching entries, **each of the plurality of topology discovery disable flags configured with a predetermined value that determines whether additional switching entries are prevented from being added to the switching database;**  
d. a global unknown destination flood control flag; and  
e. a controller implementing a secure Payload Data Unit (PDU) forwarding process whereby a received PDU having as a destination data node identifier not stored in the switching database is replicated only to physical communications ports having reset topology discovery disable flags preventing hostile data network nodes connected thereto from listening to unknown destination data traffic, **wherein implementing a**

***secure Payload Data Unit (PDU) forwarding process includes determining, from at least one of the topology discovery disable flags, whether switching entries are prevented from being added to the switching database.***

***(emphasis added)***

Applicants respectfully submit that claim 4, as amended, is allowable over the cited art for at least the reason that neither *Feldman* nor *Anderson*, alone or in combination, discloses, teaches, or suggests a “secure data switching node comprising... a plurality of topology discovery disable flags, corresponding to the plurality of switching entries, ***each of the plurality of topology discovery disable flags configured with a predetermined value that determines whether additional switching entries are prevented from being added to the switching database... wherein implementing a secure Payload Data Unit (PDU) forwarding process includes determining, from at least one of the topology discovery disable flags, whether switching entries are prevented from being added to the switching database***” as recited in claim 4, as amended. More specifically, the Office Action admits that *Feldman* “fails to teach a plurality of switching entry protection flags...” (OA page 3, element 6). For at least this reason, claim 4, as amended, is allowable.

Additionally, *Anderson* fails to overcome the deficiencies of *Feldman*. More specifically, *Anderson* discloses “[o]nce notification is received, an Internet host establishes a security authentication with an upstream router from which attack traffic is received. Once security authentication is established, the Internet host transmits one or more squelch filters to the upstream router” (page 2, paragraph [0025]). Applicants respectfully submit that this is different than claim 4, as amended, for at least the reason that the squelch filters are not transmitted to a location for implementation until after authentication is established. Consequently, *Anderson* cannot disclose determining whether additional switching entries are prevented from being added to the switching database. For at least this additional reason, claim 4, as amended, is allowable.

**D. Claim 5 is Allowable Over *Feldman* in view of *Anderson***

The Office Action indicates that claim 5 stands rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent Number 6,069,889 ("*Feldman*") in view of U.S. Publication Number 2003/0014665 ("*Anderson*"). Applicants respectfully traverse this rejection for at least the reason that *Feldman* in view of *Anderson* fails to disclose, teach, or suggest all of the elements of claim 5. More specifically, claim 5 recites:

A secure data switching node comprising:  
a. a plurality of physical communications ports;  
b. a switching database having a plurality of switching entries, each one of the plurality of switching entries specifying an association between a data network node identifier and a communications port;  
c. a plurality of unknown destination flood control flags, corresponding to the plurality of switching entries, ***each of the plurality of unknown destination flood control flags configured with a predetermined value that determines whether replication of Payload Data Unit (PDU) to communication ports is prevented***; and  
d. a controller implementing a secure Payload Data Unit (PDU) forwarding process, ***wherein implementing a secure Payload Data Unit (PDU) forwarding process includes determining, from at least one of the unknown destination flood control flags, whether replication of PDU to communication ports is prevented***, whereby a received PDU having as a destination data node identifier not stored in the switching database is replicated only to physical communications ports having reset unknown destination flood control flags preventing hostile data network nodes connected thereto from listening to unknown destination data traffic.

***(emphasis added)***

Applicants respectfully submit that claim 5, as amended, is allowable over the cited art for at least the reason that neither *Feldman* nor *Anderson*, alone or in combination, discloses, teaches, or suggests a "secure data switching node comprising... a plurality of unknown destination flood control flags, corresponding to the plurality of switching entries, ***each of the plurality of unknown destination flood control flags configured with a predetermined value that determines whether replication of Payload Data Unit (PDU) to communication ports is prevented... wherein implementing a secure Payload Data Unit (PDU) forwarding process includes determining, from at least one of the unknown destination flood control flags, whether replication of PDU to communication ports is prevented***" as recited in claim

5, as amended. More specifically, the Office Action admits that *Feldman* “fails to teach a plurality of switching entry protection flags...” (OA page 3, element 6). For at least this reason, claim 5, as amended, is allowable.

Additionally, *Anderson* fails to overcome the deficiencies of *Feldman*. More specifically, *Anderson* discloses “[o]nce notification is received, an Internet host establishes a security authentication with an upstream router from which attack traffic is received. Once security authentication is established, the Internet host transmits one or more squelch filters to the upstream router” (page 2, paragraph [0025]). Applicants respectfully submit that this is different than claim 5, as amended, for at least the reason that the squelch filters are not transmitted to a location for implementation until after authentication is established. Consequently, *Anderson* cannot disclose switching determining whether replication of PDU to communication ports is prevented. For at least this additional reason, claim 5, as amended, is allowable.

**E. Claim 6 is Allowable Over *Feldman* in view of *Anderson***

The Office Action indicates that claim 6 stands rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent Number 6,069,889 (“*Feldman*”) in view of U.S. Publication Number 2003/0014665 (“*Anderson*”). Applicants respectfully traverse this rejection for at least the reason that *Feldman* in view of *Anderson* fails to disclose, teach, or suggest all of the elements of claim 6. More specifically, claim 6 recites:

A method of securely updating a switching database of a data switching node forwarding data traffic in a data transport network, the method comprising steps of:

a. extracting a source data network node identifier from data traffic received on a source physical communications port of the data switching node;

b. querying the switching database having a plurality of switching entries, each one of the plurality of switching entries specifying an association between a data network node identifier and a communications port, the query using the extracted source data network identifier as a key, ***the switching database including a field for indicating a predetermined value associated with the source data network node identifier configured to indicate whether a new***

***switching entry is prevented from being added to the switching database;***

c. adding a new switching entry to the switching database if a switching entry corresponding to the source data network node identifier does not prevent entry to the switching database; and

d. modifying the communications port specification of a switching entry found to correspond to the extracted source data network node identifier, if a switching entry protection flag associated with the found switching entry is reset whereby preventing a redirection of data traffic processed by the data switching node.

***(emphasis added)***

Applicants respectfully submit that claim 5, as amended, is allowable over the cited art for at least the reason that neither *Feldman* nor *Anderson*, alone or in combination, discloses, teaches, or suggests a “method of securely updating a switching database of a data switching node forwarding data traffic in a data transport network, the method comprising steps of... querying the switching database having a plurality of switching entries, each one of the plurality of switching entries specifying an association between a data network node identifier and a communications port, the query using the extracted source data network identifier as a key, ***the switching database including a field for indicating a predetermined value associated with the source data network node identifier configured to indicate whether a new switching entry is prevented from being added to the switching database***” as recited in claim 5, as amended. More specifically, the Office Action admits that *Feldman* “fails to teach a plurality of switching entry protection flags...” (OA page 3, element 6). For at least this reason, claim 5, as amended, is allowable.

Additionally, *Anderson* fails to overcome the deficiencies of *Feldman*. More specifically, *Anderson* discloses “[o]nce notification is received, an Internet host establishes a security authentication with an upstream router from which attack traffic is received. Once security authentication is established, the Internet host transmits one or more squelch filters to the upstream router” (page 2, paragraph [0025]). Applicants respectfully submit that this is different than claim 5, as amended, for at least the reason that the squelch filters are not transmitted to a location for implementation until after authentication is established. Consequently, *Anderson*



cannot disclose indicating whether a new switching entry is prevented from being added to the switching database. For at least this additional reason, claim 5, as amended, is allowable.

**F. Claim 7 is Allowable Over *Feldman* in view of *Anderson***

The Office Action indicates that claim 7 stands rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent Number 6,069,889 ("*Feldman*") in view of U.S. Publication Number 2003/0014665 ("*Anderson*"). Applicants respectfully traverse this rejection for at least the reason that *Feldman* in view of *Anderson* fails to disclose, teach, or suggest all of the elements of claim 7. More specifically, claim 7 recites:

A method of securely updating data transport network topology information held in a switching database of a data switching node associated with the data transport network, the method comprising steps of:

a. extracting a source data network node identifier from data traffic received on a source physical communications port of the data switching node;

b. querying the switching database having a plurality of switching entries, each one of the plurality of switching entries specifying an association between a data network node identifier and a communications port, the query using the extracted source data network node identifier as a key, ***the switching database including a field for indicating a predetermined value associated with a topology discovery disable flag configured to indicate whether switching entries are prevented from being added to the switching database;*** and

c. adding a new switching entry to the switching database if a switching entry corresponding to the source data network node identifier is not found in the switching database and the topology discovery disable flag is reset whereby a hostile data network node is prevented from connecting to the source physical communications port.

***(emphasis added)***

Applicants respectfully submit that claim 7, as amended, is allowable over the cited art for at least the reason that neither *Feldman* nor *Anderson*, alone or in combination, discloses, teaches, or suggests a "method of securely updating data transport network topology information held in a switching database of a data switching node associated with the data transport network, the method comprising steps of... querying the switching database having a

plurality of switching entries, each one of the plurality of switching entries specifying an association between a data network node identifier and a communications port, the query using the extracted source data network node identifier as a key, ***the switching database including a field for indicating a predetermined value associated with a topology discovery disable flag configured to indicate whether switching entries are prevented from being added to the switching database***” as recited in claim 7, as amended. More specifically, the Office Action admits that *Feldman* “fails to teach a plurality of switching entry protection flags...” (OA page 3, element 6). For at least this reason, claim 7, as amended, is allowable.

Additionally, *Anderson* fails to overcome the deficiencies of *Feldman*. More specifically, *Anderson* discloses “[o]nce notification is received, an Internet host establishes a security authentication with an upstream router from which attack traffic is received. Once security authentication is established, the Internet host transmits one or more squelch filters to the upstream router” (page 2, paragraph [0025]). Applicants respectfully submit that this is different than claim 7, as amended, for at least the reason that the squelch filters are not transmitted to a location for implementation until after authentication is established. Consequently, *Anderson* cannot disclose indicating whether switching entries are prevented from being added to the switching database. For at least this additional reason, claim 7, as amended, is allowable.

**G. Claim 10 is Allowable Over *Feldman* in view of *Anderson***

The Office Action indicates that claim 10 stands rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent Number 6,069,889 (“*Feldman*”) in view of U.S. Publication Number 2003/0014665 (“*Anderson*”). Applicants respectfully traverse this rejection for at least the reason that *Feldman* in view of *Anderson* fails to disclose, teach, or suggest all of the elements of claim 10. More specifically, claim 10 recites:

A secure method of forwarding data traffic having a destination unknown to a data switching node, the method comprising steps of:

a. extracting a source data network node identifier from the unknown destination data traffic received on a source physical communications port of the data switching node;

b. querying the switching database having a plurality of switching entries each one of the plurality of switching entries specifying an association between a data network node identifier and a communications port, the query using the extracted source data network node identifier as a key, ***the switching database including a field for indicating a predetermined value associated with a global unknown destination flood control flag configured to indicate whether replication of PDU to communication ports is prevented;***

c. replicating the received data traffic to each one of a plurality of physical communications ports of the data switching node if the global unknown destination flood control flag associated with the data switching node is reset; and

d. replicating the received data traffic to each one of the plurality of physical communications ports except physical communications ports having a topology discovery disable feature set if the global unknown destination flood control flag is set whereby a hostile data network node connected to a physical communications port having the topology discovery disable flag set is prevented from spying on unknown destination data traffic.

***(emphasis added)***

Applicants respectfully submit that claim 10, as amended, is allowable over the cited art for at least the reason that neither *Feldman* nor *Anderson*, alone or in combination, discloses, teaches, or suggests a “secure method of forwarding data traffic having a destination unknown to a data switching node, the method comprising steps of... querying the switching database having a plurality of switching entries each one of the plurality of switching entries specifying an association between a data network node identifier and a communications port, the query using the extracted source data network node identifier as a key, ***the switching database including a field for indicating a predetermined value associated with a global unknown destination flood control flag configured to indicate whether replication of PDU to communication ports is prevented***” as recited in claim 10, as amended. More specifically, the Office Action admits that *Feldman* “fails to teach a plurality of switching entry protection flags...” (OA page 3, element 6). For at least this reason, claim 10, as amended, is allowable.

Additionally, *Anderson* fails to overcome the deficiencies of *Feldman*. More specifically, *Anderson* discloses “[o]nce notification is received, an Internet host establishes a security

authentication with an upstream router from which attack traffic is received. Once security authentication is established, the Internet host transmits one or more squelch filters to the upstream router” (page 2, paragraph [0025]). Applicants respectfully submit that this is different than claim 10, as amended, for at least the reason that the squelch filters are not transmitted to a location for implementation until after authentication is established. Consequently, *Anderson* cannot disclose indicating whether replication of PDU to communication ports is prevented. For at least this additional reason, claim 10, as amended, is allowable.

**H. Claim 13 is Allowable Over *Feldman* in view of *Anderson***

The Office Action indicates that claim 13 stands rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent Number 6,069,889 (“*Feldman*”) in view of U.S. Publication Number 2003/0014665 (“*Anderson*”). Applicants respectfully traverse this rejection for at least the reason that *Feldman* in view of *Anderson* fails to disclose, teach, or suggest all of the elements of claim 13. More specifically, claim 13 recites:

A secure method of forwarding data traffic having a destination unknown to a data switching node, the method comprising steps of:

a. extracting a source data network node identifier from the unknown destination data traffic received on a source physical communications port of the data switching node;

b. querying the switching database having a plurality of switching entries each one of the plurality of switching entries specifying an association between a data network node identifier and a communications port, the query using the extracted source data network node identifier as a key, ***the switching database including a field for indicating a predetermined value associated with an unknown destination flood control flag configured to indicate whether replication of PDU to communication ports is prevented;***

c. replicating the received data traffic to each one of a plurality of communications ports of the data switching node if the unknown destination flood control flags associated with the physical communications ports are reset; and

d. replicating the received data traffic to each one of the plurality of physical communications ports except physical communications ports having the unknown destination flood control flag set, whereby a hostile data network node connected to a physical communications port having the associated topology discovery disable flag set is prevented from spying on unknown destination data traffic.

**(emphasis added)**

Applicants respectfully submit that claim 13, as amended, is allowable over the cited art for at least the reason that neither *Feldman* nor *Anderson*, alone or in combination, discloses, teaches, or suggests a “secure method of forwarding data traffic having a destination unknown to a data switching node, the method comprising steps of... querying the switching database having a plurality of switching entries each one of the plurality of switching entries specifying an association between a data network node identifier and a communications port, the query using the extracted source data network node identifier as a key, **the switching database including a field for indicating a predetermined value associated with an unknown destination flood control flag configured to indicate whether replication of PDU to communication ports is prevented**” as recited in claim 13, as amended. More specifically, the Office Action admits that *Feldman* “fails to teach a plurality of switching entry protection flags...” (OA page 3, element 6). For at least this reason, claim 13, as amended, is allowable.

Additionally, *Anderson* fails to overcome the deficiencies of *Feldman*. More specifically, *Anderson* discloses “[o]nce notification is received, an Internet host establishes a security authentication with an upstream router from which attack traffic is received. Once security authentication is established, the Internet host transmits one or more squelch filters to the upstream router” (page 2, paragraph [0025]). Applicants respectfully submit that this is different than claim 13, as amended, for at least the reason that the squelch filters are not transmitted to a location for implementation until after authentication is established. Consequently, *Anderson* cannot disclose indicating whether replication of PDU to communication ports is prevented. For at least this additional reason, claim 13, as amended, is allowable.

**I. Claims 11 – 12 and 14 are Allowable Over *Feldman* in view of *Anderson***

The Office Action indicates that claims 11 – 12 and 14 stand rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent Number 6,069,889 (“*Feldman*”) in view of U.S.

Publication Number 2003/0014665 (“*Anderson*”). Applicants respectfully traverse this rejection for at least the reason that *Feldman* in view of *Anderson* fails to disclose, teach, or suggest all of the elements of claims 11 – 12 and 14. More specifically, dependent claims 11 – 12 are believed to be allowable for at least the reason that these claims depend from allowable independent claim 10. Dependent claim 14 is believed to be allowable for at least the reason that it depends from allowable independent claim 13. *In re Fine, Minnesota Mining and Mfg.Co. v. Chemque, Inc.*, 303 F.3d 1294, 1299 (Fed. Cir. 2002).

**II. Rejections Under 35 U.S.C. §103 – *Feldman* in view of *Anderson* further in view of *Civanlar***

**A. Claim 2 is Allowable Over *Feldman* and *Anderson* further in view of *Civanlar***

The Office Action indicates that claim 2 stands rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent Number 6,069,889 (“*Feldman*”) and U.S. Publication Number 2003/0014665 (“*Anderson*”) further in view of U.S. Patent Number 5,996,021 (“*Civanlar*”). Applicants respectfully traverse this rejection for at least the reason that *Feldman* and *Anderson* further in view of *Civanlar* fails to disclose, teach, or suggest all of the elements of claim 2. More specifically, dependent claim 2 is believed to be allowable over *Feldman* and *Anderson* for at least the reason that this claim depends from allowable independent claim 1. Because *Civanlar* fails to overcome the deficiencies of *Feldman* and *Anderson*, claim 2 is allowable as a matter of law. *In re Fine, Minnesota Mining and Mfg.Co. v. Chemque, Inc.*, 303 F.3d 1294, 1299 (Fed. Cir. 2002).

**B. Claims 8 – 9 are Allowable Over *Feldman* and *Anderson* further in view of *Lubarsky***

The Office Action indicates that claims 8 – 9 stand rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent Number 6,069,889 (“*Feldman*”) and U.S. Publication

Number 2003/0014665 (“*Anderson*”) further in view of U.S. Patent Number 4,893,340 (“*Lubarsky*”). Applicants respectfully traverse this rejection for at least the reason that *Feldman* and *Anderson* further in view of *Lubarsky* fails to disclose, teach, or suggest all of the elements of claims 8 – 9. More specifically, dependent claims 8 – 9 are believed to be allowable over *Feldman* and *Anderson* for at least the reason that these claims depend from allowable independent claim 7. Because *Lubarsky* fails to overcome the deficiencies of *Feldman* and *Anderson*, claim 2 is allowable as a matter of law. *In re Fine, Minnesota Mining and Mfg.Co. v. Chemque, Inc.*, 303 F.3d 1294, 1299 (Fed. Cir. 2002).

### **III. New Claims 15 – 18 are Allowable**

In addition, new claims 15 – 18 are allowable over the cited art. More specifically, claim 15 is allowable for at least the reason that this claim depends from allowable independent claim 1. Claim 16 is allowable for at least the reason that this claim depends from allowable independent claim 3. Claim 17 is allowable for at least the reason that this claim depends from allowable independent claim 4. Claim 18 is allowable for at least the reason that this claim depends from allowable independent claim 5. Claim 19 is allowable for at least the reason that this claim depends from allowable independent claim 6. Claim 20 is allowable for at least the reason that this claim depends from allowable independent claim 7. *In re Fine, Minnesota Mining and Mfg.Co. v. Chemque, Inc.*, 303 F.3d 1294, 1299 (Fed. Cir. 2002).

### **CONCLUSION**

In light of the foregoing amendments and for at least the reasons set forth above, Applicants respectfully submit that all objections and/or rejections have been traversed, rendered moot, and/or accommodated, and that the now pending claims are in condition for allowance. Favorable reconsideration and allowance of the present application and all pending claims are hereby courteously requested.

Any other statements in the Office Action that are not explicitly addressed herein are not intended to be admitted. In addition, any and all findings of inherency are traversed as not having been shown to be necessarily present. Furthermore, any and all findings of well-known art and Official Notice, or statements interpreted similarly, should not be considered well-known for the particular and specific reasons that the claimed combinations are too complex to support such conclusions and because the Office Action does not include specific findings predicated on sound technical and scientific reasoning to support such conclusions.

If, in the opinion of the Examiner, a telephonic conference would expedite the examination of this matter, the Examiner is invited to call the undersigned attorney at (770) 933-9500.

Respectfully submitted,

/afb/

**Anthony F. Bonner Jr. Reg. No. 55,012**

**THOMAS, KAYDEN,  
HORSTEMEYER & RISLEY, L.L.P.**  
Suite 1500  
600 Galleria Parkway N.W.  
Atlanta, Georgia 30339  
(770) 933-9500